February 29, 2007

Chairman Kevin Martin
Federal Communications Commission
445 12th Street SW
Room #8B-201
Washington, DC 20554

RE: WT Docket 07-16 & 07-30
        M2Z's Network Level Filtered Wireless Broadband Service

Dear Chairman Martin,

       I am writing to you on behalf of the iKeepSafe Internet Safety Coalition. Our coalition of business leaders, non-profit advocates and public policy makers was formed with the singular goal of helping parents, educators and caregivers keep America's children safe on the Internet. Today our coalition includes the Governors or First Spouses of 49 states and over 50 corporate and association partners including the National Center for Missing and Exploited Children, the National PTA and the American Medical Association. This breadth of experience and expertise allows us to prepare and disseminate educational tools and programming that are helping children stay safe online all across the United States and around the world. As part of our mission to help parents, educators, and caregivers teach children the safe and healthy use of technology and the Internet we are constantly searching for new tools to assist in that endeavor. Thus, we were very excited to learn of the proposal of M2Z Networks to provide a network level filtered wireless broadband Internet service. The iKeepSafe Coalition applauds this great initiative and we hope that other industries follow in creating safe solutions for parents and families.

       The need for a variety of tools to keep children safe online has never been greater. A study from the Office of Juvenile Justice and Delinquency Prevention from 2005 reported that from 2004 to 2005 there was an 84% rise in the number of formal complaints that predators had enticed minors online or traveled to meet them in person. The Polly Klaas Foundation reported in 2006 that 56% of teens receive requests for personal information online. Most significantly, the University of New Hampshire reported in 2001 that 1 in 4 children are inadvertently exposed to online pornography every year. These frightening statistics underscore the need to arm parents, educators and caregivers with a greater and more effective array of tools in the fight to keep children safe online.

       At iKeepSafe, we have focused on teaching safe behaviors. In addition to countless other programs and efforts, we have produced two volumes in the Faux Paw the Techno Cat Internet Safety Program. In the first book Faux Paw, the Governor's curious cat, gets into trouble when she agrees to meet a chat room "friend." Through the course of the book children learn the safety guidelines integrated into the story. The messages in

the book can be reinforced by an interactive website, in-school presentation materials and an animated, student Emmy Award winning movie. In a second volume published in 2006, First Lady Laura Bush teaches Faux Paw how to avoid and handle cyber-bullying as it reinforces the basic rules of Internet safety. We also have made available on our website www.ikeepsafe.org a handbook to help parents stay in control of their computers and their children activities online. We have enclosed that document "10 Technical Questions: What Every Parent Must do to Keep Children Safe Online," with this letter for your information.

Keeping children safe online is a multi-layered endeavor. Thus, we recognize that no one tool or educational program will address all of the concerns. That is why the iKeepSafe Coalition is vigilant about providing a whole host of tools and technologies to help parents, educators and caregivers manage the challenging task of keeping unwanted, harmful and illegal materials away from our children as they take advantage of all the wonders on the Internet. For that reason, we herald the proposal of M2Z Networks to provide a network level filtered wireless broadband Internet service. As you know, network level filters are superior to those housed on individual computers as they cannot be easily circumvented by technologically savvy users. This is because indecent content will be blocked by M2Z before it ever reaches the user's computer thus eliminating one of the most common avenues for the online solicitation of minors: indecent websites. This type of filtering is one of the best tools we have to fend off online predators. Moreover, the filter will help both parents who are unfamiliar and uncomfortable with the role of being the home IT Administrator and those that are dedicated and committed to that task because the reality is that children cannot be monitored at every moment when online. We believe that if more service providers were to follow M2Z's lead, it would significantly help parents and other caregivers keep our children safe online.

Astonishingly, M2Z has not only taken the lead in this area, but it has also committed to do it quickly. The company has agreed to provide this service to 95% of the American people within 10 years, with interim benchmarks of 33% of the population in 3 years and 66% in five years. iKeepSafe believes that the availability of a service like that proposed by M2Z Networks will be an invaluable tool in the fight to keep children safe online. I urge you to seriously consider this proposal, and take all actions that will give parents across the country a broadening array of tools they can use to protect their Children.

Sincerely,

Marsali S. Hancock
President
Internet Keep Safe Coalition
5220 36th St N
Arlington, VA 22207

Enclosure: 10 Technical Questions: What Every Parent Must do to Keep Children Safe Online

cc: Commissioner Michael J. Copps
Federal Communications Commission

Commissioner Jonathan S. Adelstein
Federal Communications Commission

Commissioner Deborah Taylor Tate
Federal Communications Commission

Commissioner Robert M. McDowell
Federal Communications Commission

Fred Campbell
Chief, Wireless Telecommunications Bureau
Federal Communications Commission

10 Common Questions About Internet Safety

Spyware, online fraud, and other Internet threats are certainly not new. But they are growing more sophisticated and criminal every day.

So how can you protect your children against these online dangers? And how can you provide a safe, appropriate Internet environment in the face of online criminals who know more about technology than you ever will?

Fortunately, there are good answers to these tough questions—thanks to a large, capable group of people and resources dedicated to helping you keep the Internet safe.
With only a little effort on your part, you can educate yourself…

Tap into the world's best resources for finding, monitoring, and defending your children against online threats….
And start using the Internet more safely and confidently.

Your part is straightforward.
• Just learn the right answers to these 10 common questions about Internet technology…
• Teach your children safe surfing practices…
• And take some easy steps to protect your computer.

1.   How and why do I check the Web browser history?

2.   How and why do I review temporary Internet files?

3.   How and why do I remove spyware?

4.   How and why do I scan for and remove viruses?

5.   How and why do I use a firewall?

6.   How do I monitor and block incoming files and information from the Internet?

7.   How do I monitor and block outgoing files and information?

8.   How do I adjust search engine settings (i.e. Google preferences)?

9.   What safety and security tools are available on a typical home computer?

10.   What are "updates" and why should I install them?

## 1. How and why do I check the Web browser history?

The Basics:

- The Web browser history lists the Web sites your child has visited recently.
- It's a useful resource for checking Internet activity.
- Web browser histories are easy to change and delete, so they are not foolproof.

To check the Web browser history in Internet Explorer, click the History icon.
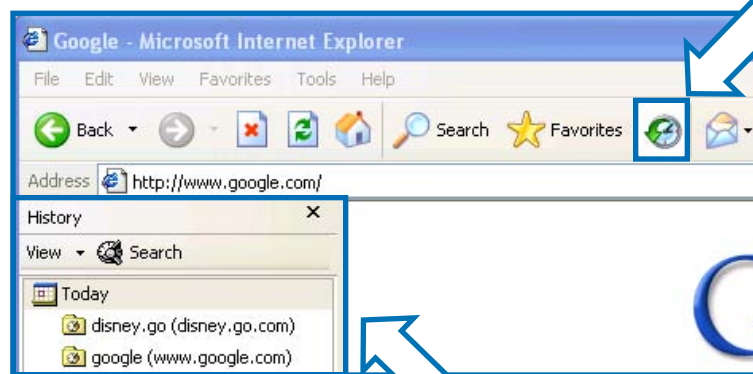
This opens a History pane on the left side of your browser window that displays a list of recently visited sites.

You can click any item on the list for more detailed information.
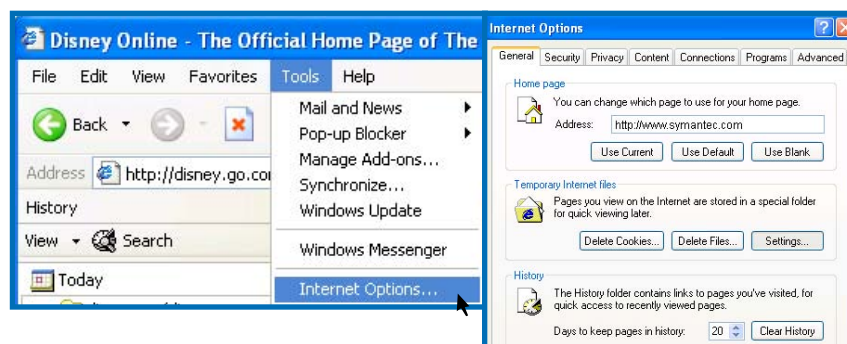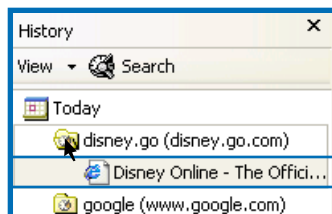
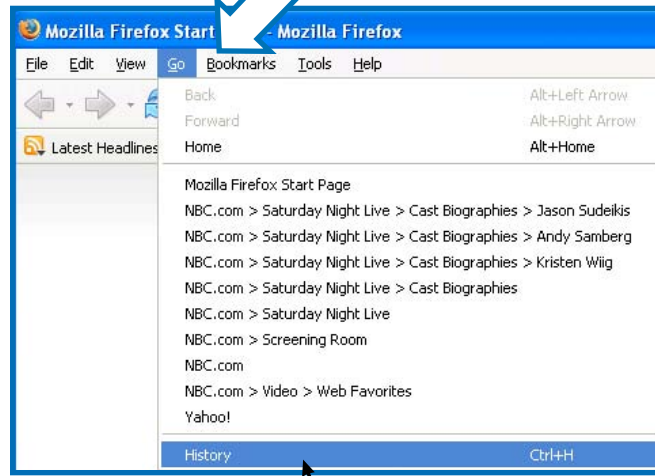You can also access additional browser history options by selecting Internet Options from the Tools menu.

Other browsers have similar browser history features that are generally very easy to access.

2. How and why do I review temporary Internet files?

The Basics:

- Your Web browser creates temporary files automatically to speed up your Internet experience.
- These files can include Web pages, images, sound files, or movies.
- Although the number and variety of temporary Internet files can be intimidating, examining them provides a very detailed view of exactly what your children have been viewing online.
- You should check temporary Internet files if there are unusual or suspicious holes in your child's browser history.
- Like the browser history, Internet-savvy children or teens can delete temporary Internet files fairly easily.

To view temporary Internet files in Internet Explorer, select Internet Options from the Tools menu.
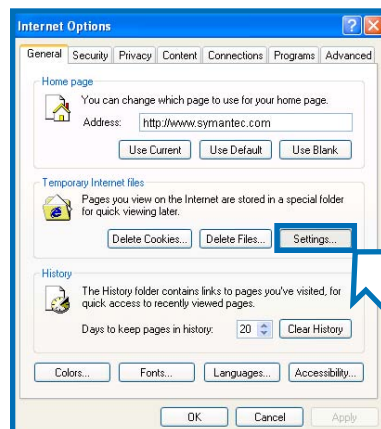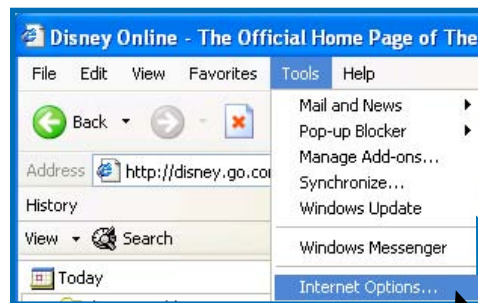
Click the Settings button found in the Temporary Internet Files section of the Internet Options window.

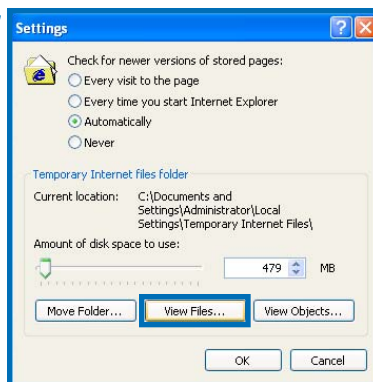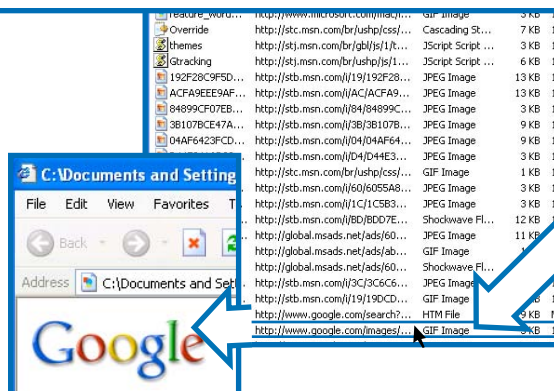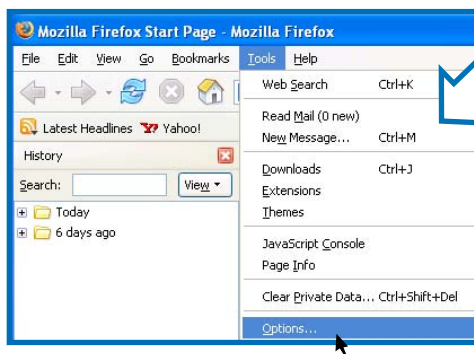Next, click the View Files button to see a list of all the temporary Internet files stored on your computer. Double click any file to see what it contains.

Settings

Check for newer versions of stored pages:
- ○ Every visit to the page
- ○ Every time you start Internet Explorer
- ● Automatically
- ○ Never

Temporary Internet files folder

Current location: C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\

Amount of disk space to use:

479   MB

Move Folder...   View Files...   View Objects...

OK   Cancel

Temporary Internet Files
File   Edit   View   Favorites   Tools   Help

For example, clicking on a file with a .gif extension will display an image that was part of a recently viewed Web site.

feature_word...	http://www.microsoft.com/mac/i...	GIF Image	3 KB
Override	http://stc.msn.com/br/ushp/css/...	Cascading St...	7 KB
themes	http://stj.msn.com/br/gbl/js/1/t...	JScript Script ...	3 KB
Gtracking	http://stj.msn.com/br/ushp/js/1...	JScript Script ...	6 KB
192F28C9F5D...	http://stb.msn.com/i/19/192F28...	JPEG Image	13 KB
ACFA9EEE9AF...	http://stb.msn.com/i/AC/ACFA9...	JPEG Image	13 KB
84899CF07EB...	http://stb.msn.com/i/84/84899C...	JPEG Image	3 KB
3B107BCE47A...	http://stb.msn.com/i/3B/3B107B...	JPEG Image	9 KB
04AF6423FCD...	http://stb.msn.com/i/04/04AF64...	JPEG Image	9 KB
	http://stb.msn.com/i/D4/D44E3...	JPEG Image	3 KB
	http://stc.msn.com/br/ushp/css/...	GIF Image	1 KB
	http://stb.msn.com/i/60/6055A8...	JPEG Image	3 KB
	http://stb.msn.com/i/1C/1C5B3...	JPEG Image	3 KB
	http://stb.msn.com/i/BD/BDD7E...	Shockwave Fl...	12 KB
	http://global.msads.net/ads/60...	JPEG Image	11 KB
	http://global.msads.net/ads/ab...	GIF Image	
	http://global.msads.net/ads/60...	Shockwave Fl...	
	http://stb.msn.com/i/3C/3C6C6...	JPEG Image	
	http://stb.msn.com/i/19/19DCD...	GIF Image	
	http://www.google.com/search?...	HTM File	5 KB
	http://www.google.com/images/...	GIF Image	8 KB

C:\Documents and Setting
File   Edit   View   Favorites

Back

Address   C:\Documents and Set

Google

Most popular browsers include a similar View Temporary Files option.

Mozilla Firefox Start Page - Mozilla Firefox
File   Edit   View   Go   Bookmarks   Tools   Help

Latest Headlines   Yahoo!

History

Search: View ▾

- ⊞ Today
- ⊞ 6 days ago

Tools menu:
- Web Search   Ctrl+K
- Read Mail (0 new)
- New Message...   Ctrl+M
- Downloads   Ctrl+J
- Extensions
- Themes
- JavaScript Console
- Page Info
- Clear Private Data... Ctrl+Shift+Del
- Options...

3. How and why do I remove spyware?

The Basics:

- Generally speaking, spyware is software that hides on your computer, tracks what you're doing online, and then sends that information over the Internet.
- Some types of spyware, called "keystroke loggers" actually record and send everything you type on your computer.
- Spyware software can sneak onto your computer when you download unsafe software and files—or even visit a hostile Web page.
- One major source of spyware is the peer-to-peer file sharing software commonly used to share music and videos online.

Tips for avoiding spyware and adware:

- Set concrete ground rules with your children. Specify exactly what they are allowed (and not allowed) to do online.
- Keep your PC in a public part of the house, where you can monitor your children's online activities.
- Avoid clicking on banner ads, links, or offers that appear too good to be true.
- Be cautious with file-sharing software and other potentially unwanted software.
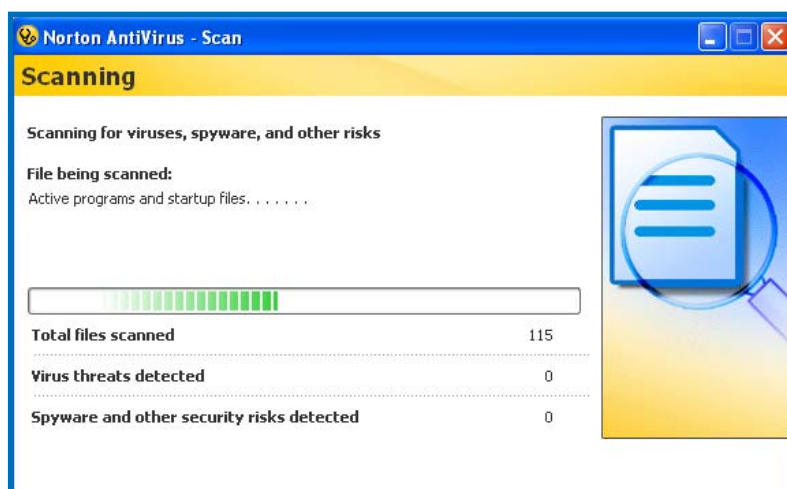
A quality Internet security program will scan your computer for spyware, adware, Trojan Horse programs, and other Internet risks...
And remove any malicious or unwanted software it finds.

Many Internet security companies also offer free online scanning services to detect spyware, adware and malicious programs.

4. How and why do I scan for and remove viruses?

The Basics:

- Viruses are software programs that hide on your computer and cause mischief or damage.
- Viruses are also called worms, Trojan Horse programs, or other names, depending on how they behave. Together, all this malicious software is commonly referred to as "malware."
- Around 80% of malware today is designed to find and steal confidential information stored on your computer. This type of malware is sometimes called "crimeware."
- Malware can invade your machine through infected email attachments, "bots" that crawl the Internet looking for unprotected computers, and visits to "hostile" Web sites.

Protecting your computer from malware isn't difficult. But it does require a quality antivirus or Internet security program.

After you install your antivirus program, make sure the automatic protection feature is turned on. This will block malware the moment it attempts to creep onto your system.
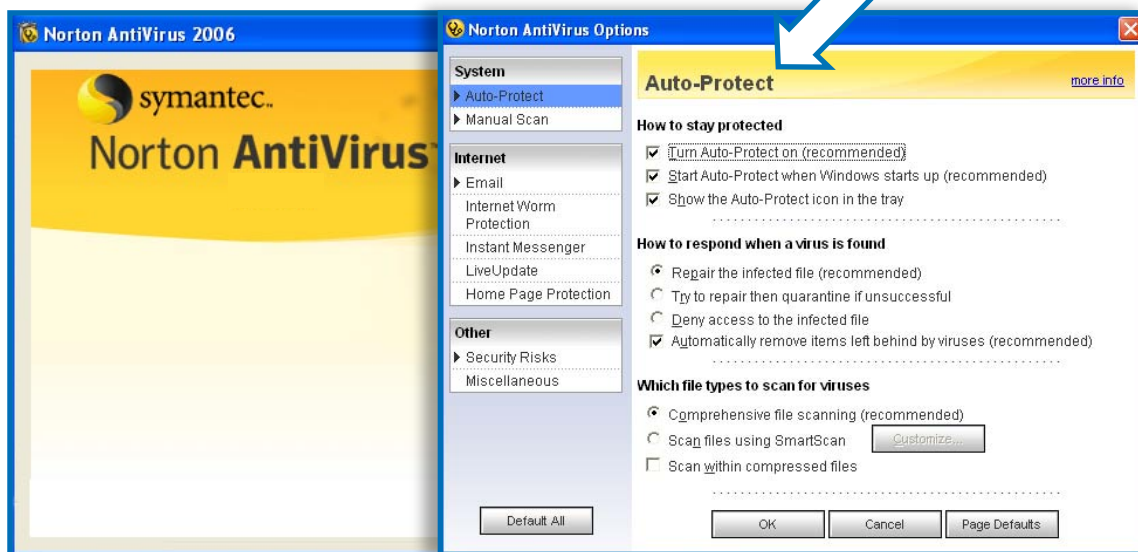
It's also important to scan your system for malware regularly. Most antivirus programs include two types of scans: a faster "quick scan" and a slower, more thorough "full system scan."

Scan Now

Scan your computer for spyware, viruses and other security risks.

◉ Full System Scan
A comprehensive scan of your entire computer.

◯ Norton QuickScan
A fast scan of the areas of your computer that are most likely to be affected.

Perform quick scans frequently to get a fast status report on the health of your PC. The quick scan option will search for malware where it hides most frequently.

Scanning

Scanning for viruses, spyware, and other risks

File being scanned:
Active programs and startup files. . . . . . .

Total files scanned	115
Virus threats detected	0
Spyware and other security risks detected	0

At least once a week, take the time to perform a full system scan. This option conducts a thorough scan of every file on your computer.

Because full system scans take longer, most people schedule them to run when the computer is idle. Scheduling full systems scans is an easy and straightforward process.
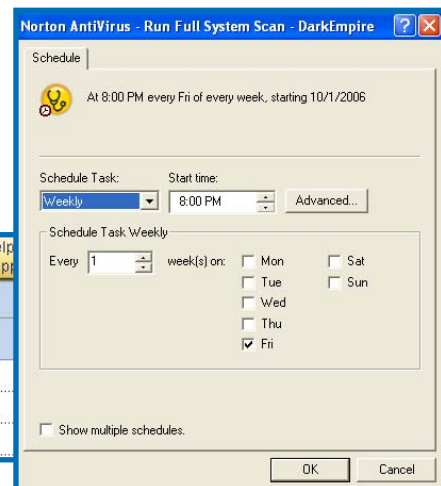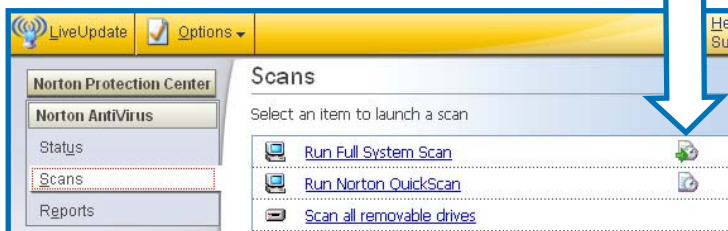
LiveUpdate Options ▾   Help Supp

Norton Protection Center

Norton AntiVirus

Status

Scans

Reports

Scans

Select an item to launch a scan

🖥 Run Full System Scan
🖥 Run Norton QuickScan
🖥 Scan all removable drives

Norton AntiVirus - Run Full System Scan - DarkEmpire

Schedule

At 8:00 PM every Fri of every week, starting 10/1/2006

Schedule Task: Start time:
Weekly ▾   8:00 PM   Advanced...

Schedule Task Weekly
Every 1   week(s) on: ☐ Mon   ☐ Sat
                        ☐ Tue   ☐ Sun
                        ☐ Wed
                        ☐ Thu
                        ☑ Fri

☐ Show multiple schedules.

OK   Cancel

It's also very important to keep your antivirus software up-to-date, since new malware is being released every day.

Most antivirus programs download updates automatically. Just make sure these updates are happening—and that your subscription stays current.
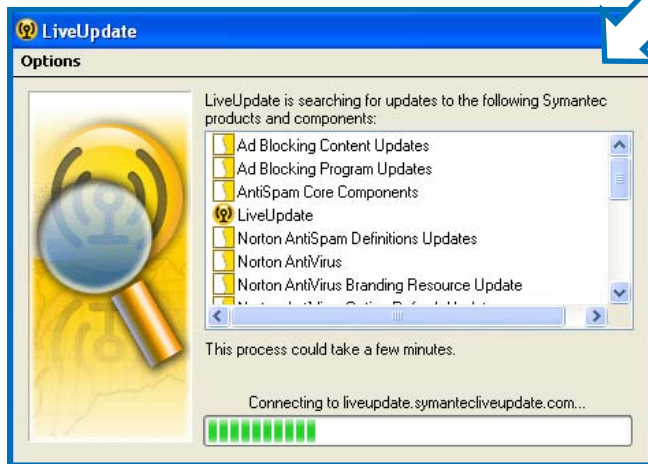
5. How and why do I use a firewall?

The Basics:

- A firewall is your main line of defense against hackers, identity thieves, and other online predators.
- It monitors all the data flowing in and out of your computer—and automatically blocks harmful traffic.
- There are so many hackers looking for "fresh" unprotected machines that you should NEVER connect to the Internet without a firewall installed.
- Firewalls can be purchased separately—or as part of an Internet Security "suite" that typically includes firewall, antivirus, anti-spyware, anti-spam, and parental control software.
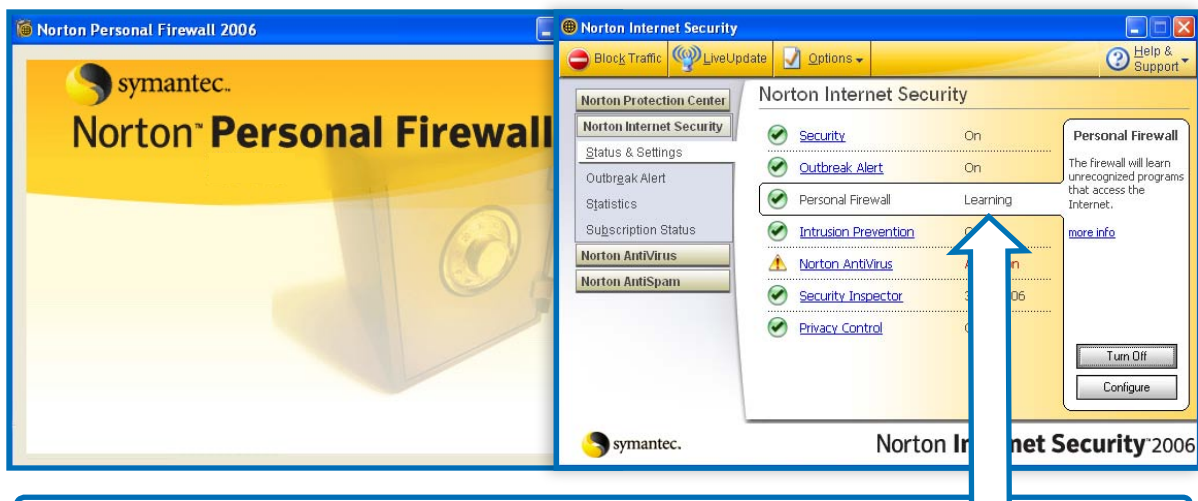
From the moment you install and activate your firewall software, it begins to "learn" about what programs you use online.

As part of this process, you may receive occasional messages from the software asking you whether you would like to block, allow, or temporarily allow different programs to use your Internet connection.
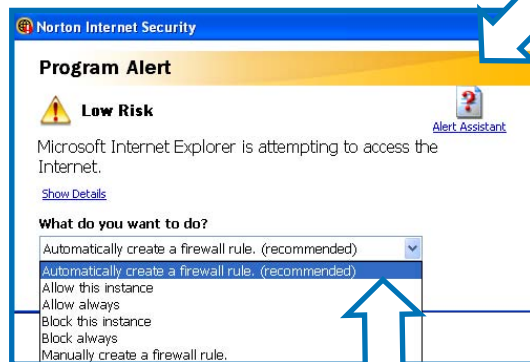
These questions will include advice from the software. In most cases, the best course of action is to simply follow the recommendation.

It's important to keep your firewall software current and up-to-date.
Most firewalls download these updates automatically. Just make sure updates are taking place regularly—and that your subscription stays current.
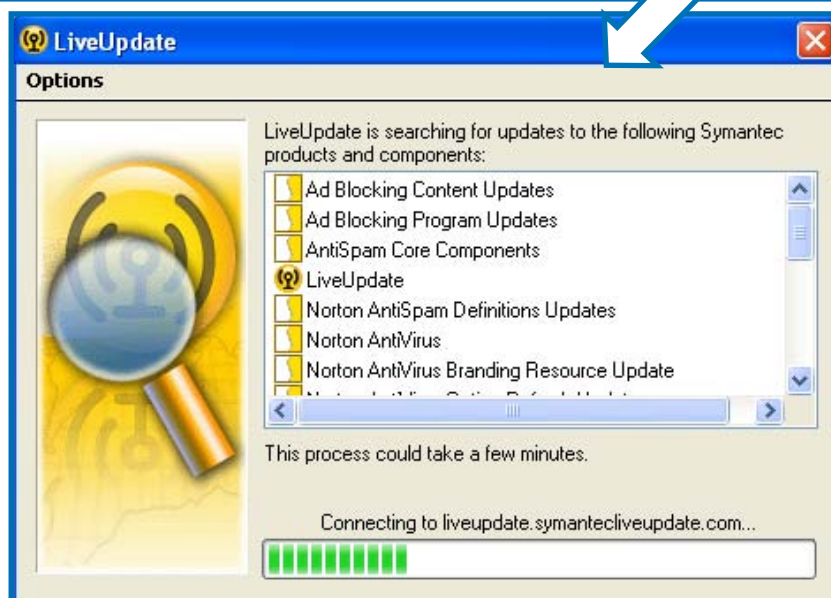
6. How do I monitor and block incoming files and information from the Internet?

The Basics:

- Three main types of security software can help you monitor and block harmful files from the Internet: firewalls, antivirus software, and intrusion detection programs.
- A firewall monitors the information coming into your computer for suspicious activity.
- Antivirus software "unwraps" incoming files and examines them for viruses, worms, and other threats.
- Intrusion detection programs block attacks that try to take advantage of security holes in common applications such as Internet Explorer.

For the most complete protection against dangerous incoming files, start by installing and activating a quality firewall program.
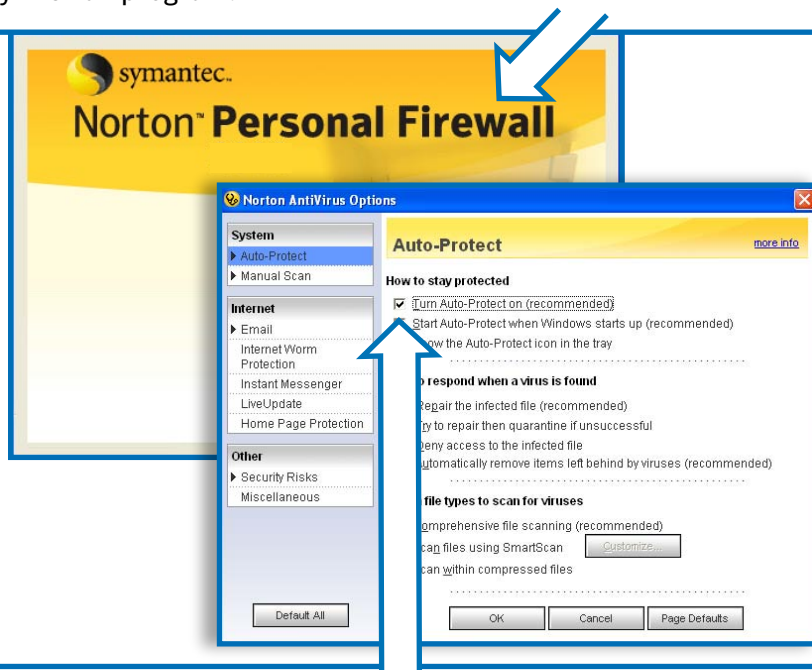
Next, make sure the AutoProtect feature in your antivirus program is turned on—and that your antivirus software is current and up-to-date.

Finally, install a program with intrusion prevention features to shield your computer from attackers who may try to take advantage of security flaws in Internet Explorer and other programs.
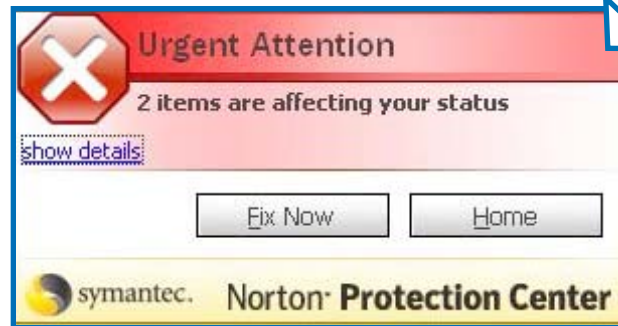
Many Internet security companies offer security "suites" that provide all of these capabilities in one easy-to-use, integrated package.
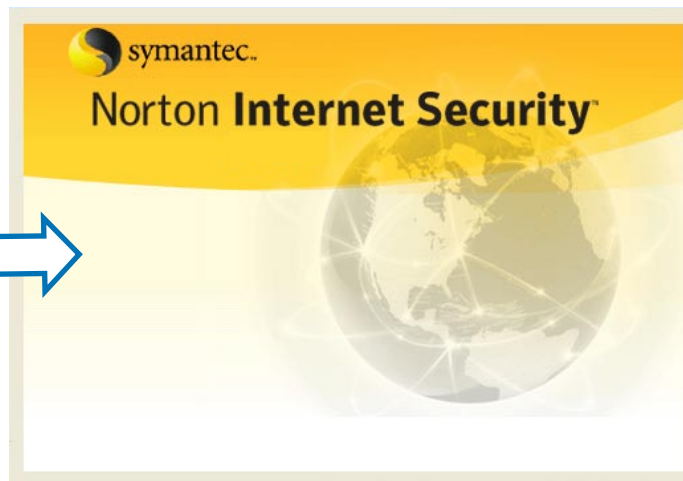
AntiVirus

Firewall

Parental Controls

AntiSpam

Privacy Controls

7. How do I monitor and block outgoing files and information?

The Basics:

- It's very important to keep sensitive personal information from "leaking" onto the Internet.
- This can happen when personal information is sent from your computer over the Internet.
- Without proper precautions, people can use instant messaging programs to remove sensitive information from your computer.
- File-sharing or peer-to-peer networking programs such as Kazaa, Limewire, and Bit Torrent can also make it easier for people to access sensitive files on your computer.

To prevent people from accessing and removing sensitive information from your computer, start by installing a firewall program that alerts you whenever private information is about to be transmitted over the Internet.

Next, configure your instant messaging program to block anyone from downloading files from your computer.
In Yahoo Instant Messenger, select Preferences from the Messenger menu, select File Transfer from the list, and choose "Never allow others to download files from me."
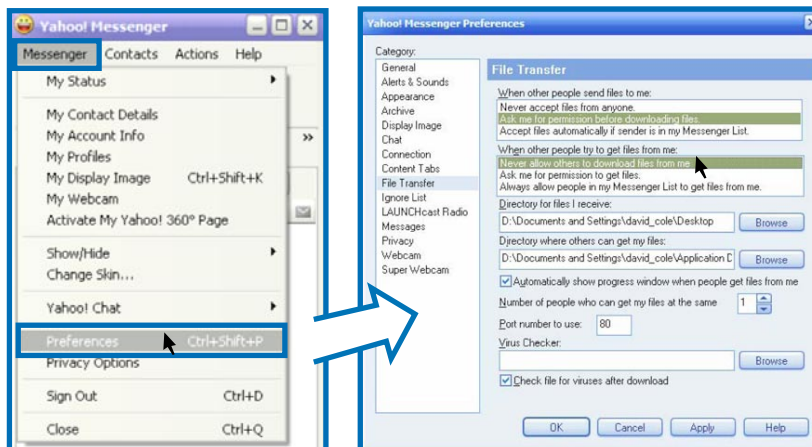
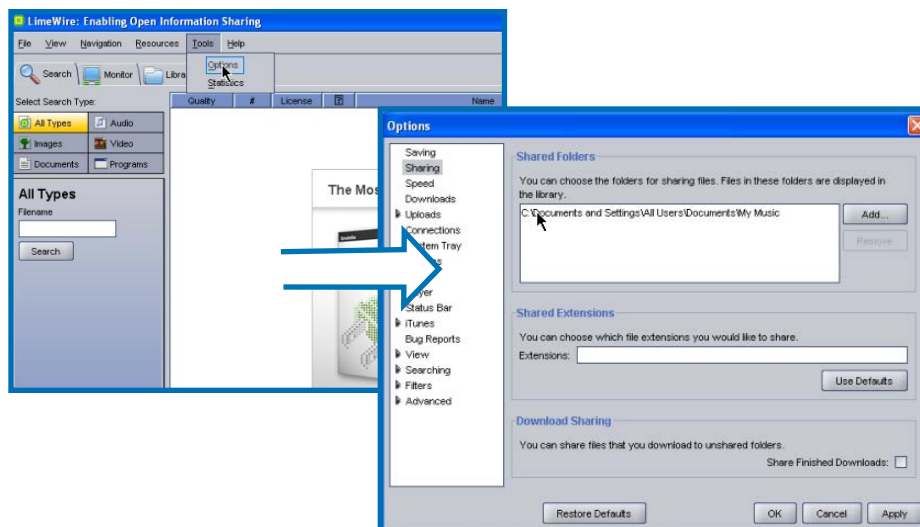Other instant messaging programs have similar options—usually found under the Preferences menu.

Finally, if you use a peer-to-peer file-sharing program, be sure to specify one folder for exchanging files. Too many people accidentally share their whole hard drive, which exposes all the files on your machine to anyone using the same file-sharing program.
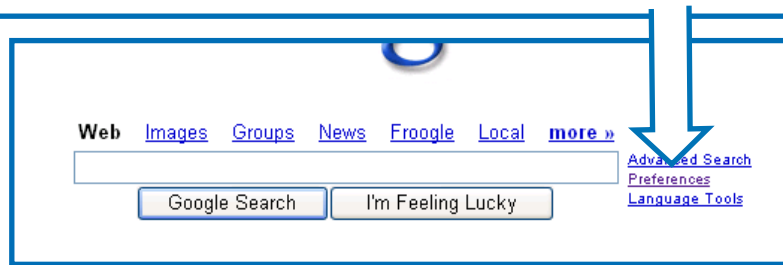
8. How do I adjust search engine settings (i.e. Google preferences)?

The Basics:

- Search engines can provide children with fast, easy access to inappropriate material on the Internet.
- Most search engines allow you to block search results that are unsuitable for children.
- Blocking inappropriate search results greatly reduces the chance that your children will stumble across dangerous or objectionable material on the Internet.
- These search result filters are not foolproof—some unwanted content may still appear in the search results.

To block inappropriate search results in Google, click Preferences from the main Google home page.

| Web | Images | Groups | News | Froogle | Local | **more »** |

Advanced Search
Preferences
Language Tools

Google Search   I'm Feeling Lucky

Next, scroll down to SafeSearch Filtering and select the Use Strict Filtering option. This will block search results with explicit text or images.

SafeSearch Filtering

...gle's SafeSearch blocks web pages containing explicit s... ...earing in search results.

⦿ Use strict filtering (Filter both explicit text and explicit im...
○ Use moderate filtering (Filter explicit images only - defau...
○ Do not filter my search results.

Yahoo! and most other popular search engines offer a similar filtering function.

None of these filtering features are 100% accurate—and some unsuitable content may still slip through.
That's why it's important to teach your children to surf the Web safely—and take the time to explore the Internet with them.

## 9. What safety and security tools are available on a typical home computer?

The Basics:

- Most home PCs run Microsoft Windows XP, which includes a number of important basic Internet security capabilities.
- The Windows Security Center provides important basic information about your computer's security status.
- Add-on Internet security products can offer more advanced, complete protection against Internet threats.

To access the Windows Security Center, open your Windows Control Panel and select Security Center.
The Security Center will tell you whether your antivirus and firewall programs are installed and working properly—and whether you are receiving automatic software updates.
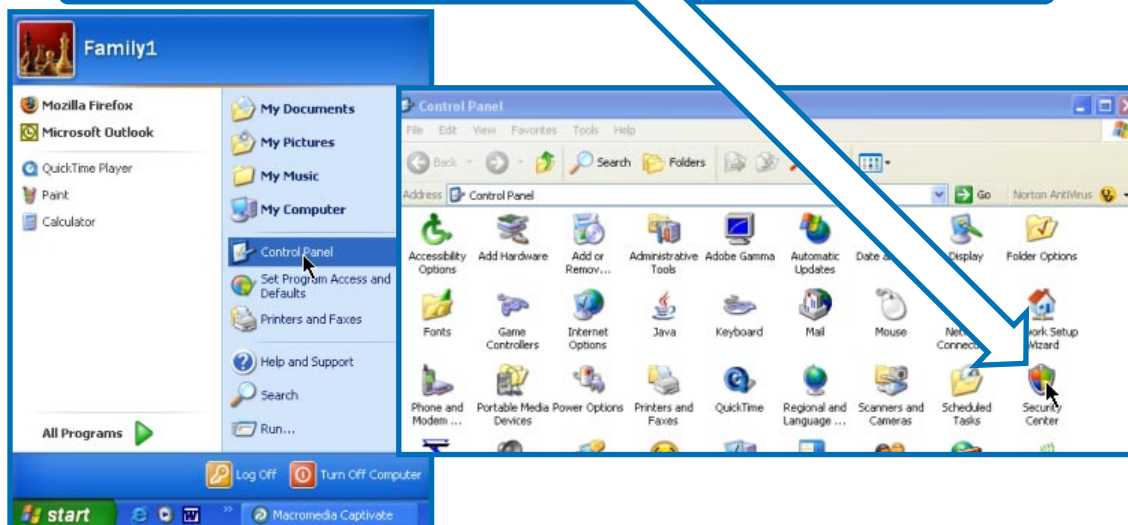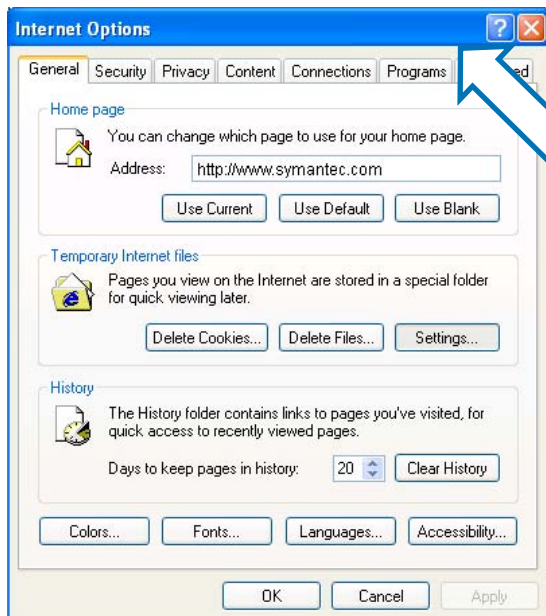
Microsoft Windows XP also includes an Internet Options control panel that allows you to manage important privacy settings.

This includes the ability to specify what types of cookies can be placed on your machine by different Web sites.

In many cases, cookies are harmless files that allow Web sites to remember your name or perform other useful functions.

But some cookies track your behavior online and can affect your privacy, so some level of control is advisable.

To change your Internet privacy settings, open your Windows Control Panel, select Internet Options, and click the Privacy tab.
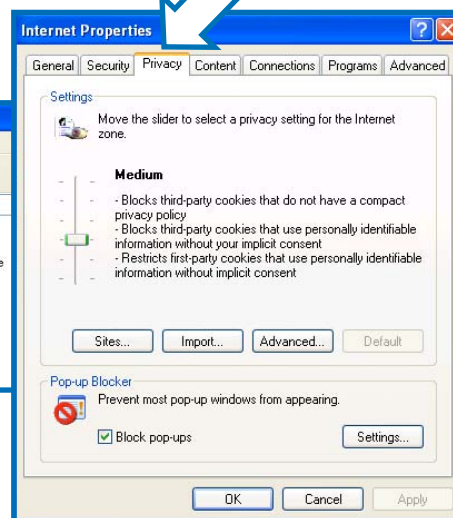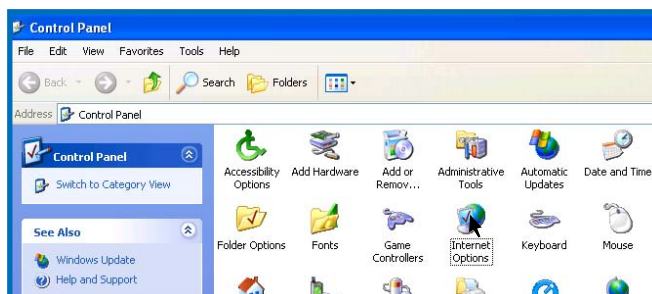
10. What are "updates" and why should I install them?

The Basics:

- Updates—also called patches—are fixes or enhancements to the software running on your computer.
- Often, patches repair security "holes" in software that may be used by hackers to attack your PC.
- Other updates may keep your security software up-to-date with the latest information about new Internet threats.
- Updates are released regularly by software companies like Microsoft, Symantec, Adobe, and others.
- You should always apply updates as soon as they become available. Running the most up-to-date software makes it much more difficult for hackers to gain access to your computer.

Microsoft software includes an "auto-update" feature that downloads and applies the latest software updates automatically.

To activate auto-update in Microsoft Windows XP, open your Windows Control Panel and click Automatic Updates. Select the "Automatic" option to update your computer automatically.
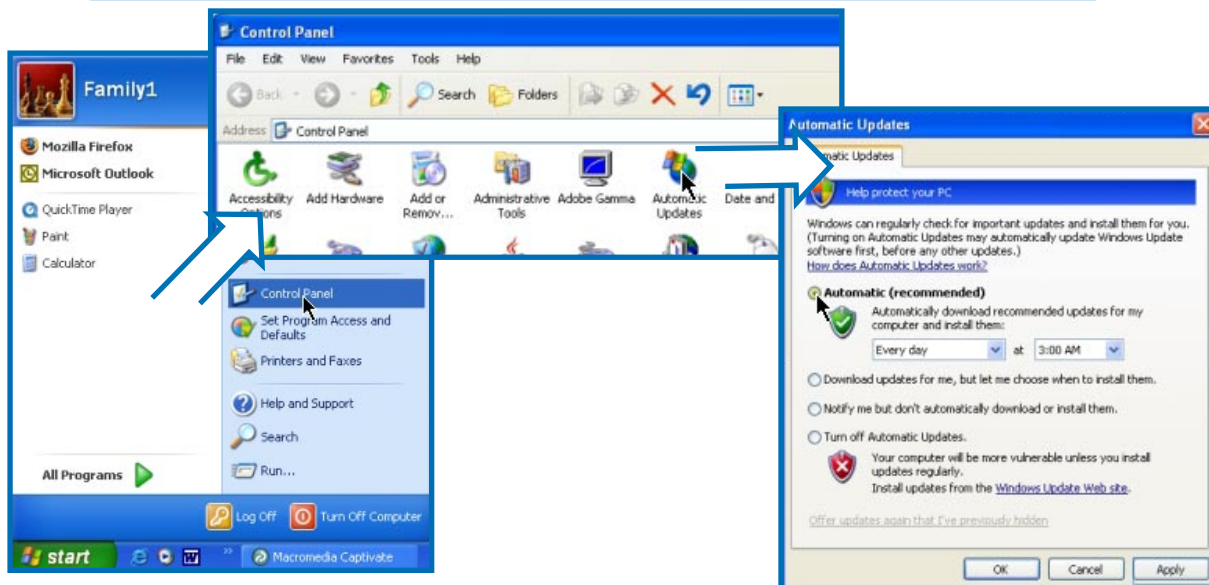
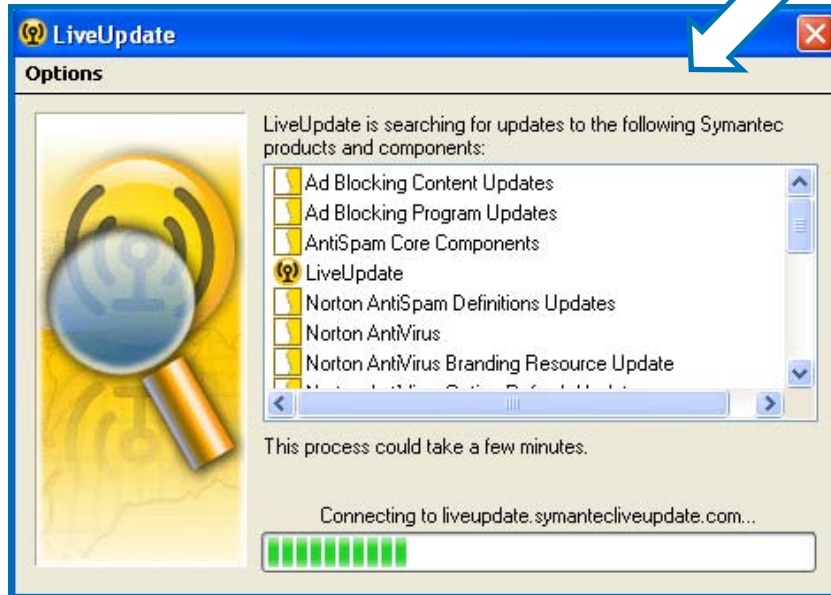Most security software also includes a feature that automatically downloads updates and information needed to detect and eliminate the latest viruses, worms, and other Internet threats.

Keeping your family safe from online threats doesn't have to be difficult or intimidating.

Just become familiar with the answers to these questions…

Follow a few simple, common-sense rules…

And start using the world's leading Internet experts to protect your home PC against today's most sophisticated Internet threats.